MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2018/2019

TMI 3231 – MALWARE AND INTRUSION DETECTION

(All sections / Groups)

27 October 2018
2.30pm – 4.30pm
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 4 pages with 5 Questions including the cover page.
2. Attempt **ALL FIVE** questions. All questions carry equal marks and the distribution of the marks for each question is given.
3. Please print all your answers in the Answer Booklet provided.

QUESTION 1

a) "Residual risk" is a key term in information security. Define the meaning of this term "Residual risk" and provide any **FOUR (4)** ways to control risk.

(4 marks)

b) A new website is launched for customers to order the custom-made cakes. However, there occurs a sudden increase of computer attacks to the website. After a thorough inspection, you identified that the attack might be Denial-of-service (DoS) attack or Distributed denial-of-service (DDoS). Explain how these two attacks work differently.

(4 marks)

c) During a typical crimeware attack, crimeware is distributed to infect a computer platform. Then the crimeware will execute. Describe any **FOUR (4)** potential attacks after a crimeware is executed.

(4 marks)

QUESTION 2

a) Keylogger is one of the popular malicious software threats. There are two types of Keyloggers: Software Keyloggers and Hardware Keyloggers. Differentiate between these two attacks.

(4 marks)

b) A computer virus exhibits three characteristics: replication mechanism, activation mechanism and objective mechanism. Discuss briefly the differences among these three characteristics.

(3 marks)

c) Files in your company's computer system have been infected by the virus. After inspection, the files are found to be infected by two types of viruses, which are appending viruses and amoeba infection viruses. In order to log a detailed report to your manager, explain how these viruses work to infect the files. Also, suggest a solution on detecting system file alterations.

(3 marks)

d) Social engineering is one of the most popular forms of attack. Identify **TWO (2)** social engineering tactics that can be used to target online bank customers.

(2 marks)

Continued...

QUESTION 3

a) Firewalls have become ubiquitous across the enterprise IT landscape because of their proven ability in security tasks. Identify any **SIX (6)** security tasks of firewalls.

(3 marks)

b) Your company would like to know more about firewalls. You, as an IT expert, are asked to list and explain these **FIVE (5)** major processing-mode categories of firewalls.

(5 marks)

c) Mr Tan would like to purchase a stateful packet filter to protect his home network. However, he was told that stateful packet filter has some well-documented limitations. If you are Mr Tan, how do you explain these limitations?

(2 marks)

d) What type of data can an attacker insert into a TCP header to fool a stateless packet filter?

(2 marks)

QUESTION 4

a) ABC Sdn Bhd understands that it is important to ensure the critical resources for a firewall's successful operation. Certain performance considerations are needed in order to increase the productivity of a firewall. As an IT administrator, you are to suggest any **FOUR (4)** examples of performance considerations.

(2 marks)

b) You are asked to setup with a screened-host system and you understand that the screened-host firewall is a more flexible firewall than the dual-homed host firewall. Discuss to your team on how the flexibility and security can be achieved by the screened-host firewall.

(3 marks)

c) Why do proxy server reassemble packets before sending them on their way to the dedicated server?

(3 marks)

Continued...

d) Proxy server originally developed as a way to speed up communications on the web by storing site's most popular pages in cache. Since then, it becomes a security solution. What are the benefits of proxy servers in network security?

(4 marks)

QUESTION 5

a) When configuring a bastion host, it is advisable not to use the production server for testing. In this case, how would you test your configuration?

(3 marks)

b) A bastion host provides only one network service, and that service is a firewall. True or False? Justify your answer.

(2 marks)

c) Intrusion Detection System (IDS) can be classified by the detection method that is employed. Describe **TWO (2)** detection methods that are used in IDS.

(3 marks)

d) Mary is worried about the attacks on cryptosystems especially Correlation attacks and Timing attacks, which are commonly launched by attackers. How do these two attacks work?

(2 marks)

e) A remote access connection is needed if users in disparate locations need to connect to the central network via a Virtual Private Network (VPN). How can you enable a remote user to connect to a VPN?

(2 marks)

End of Paper